Icon Training - Data Protection Policy

Introduction

You may be aware that the EU has introduced a new law called the General Data Protection Regulation, or GDPR. This new law has introduced significant enhancements to the old Data Privacy Directive. You are aware that our organisation is dependent on using the Personal Data of individuals. The GDPR also calls these 'individuals', Data Subjects.

As an employee, you are a Data Subject and we use your Personal Data such as your name, identification, address and banking details; or perhaps sensitive data such as your health status or trade union membership. Our clients and customers are also Data Subjects. The GDPR states that this Personal Data must be protected, it must remain fresh and valid and that Data Subjects must be able to access their Personal Data.

Requirements

We expect our leadership to:

- Understand the requirements of the GDPR, especially for areas under their influence and especially where they have responsibilities as Information Owners
- Drive the adoption of the appropriate behaviours throughout our organisation
- Understand and regularly assess and respond to any privacy risk to their areas of operation

Policy Statement

This Policy defines the responsibilities and expected behaviours of all our Employees, Contractors and relevant Organisation Partners which will uphold a Data Subject's right to have his or her Personal Data processed in accordance with the requirements of the General Data Protection Regulation.

Scope

This Policy applies to:

- the Personal Data of all Data Subjects with whom we interact during the normal course of our organisation
- all types of and uses for Personal Data within our organisation
- all our employees and organisation partners, especially those who deal directly with Personal Data
- all our organisation's processes and all systems (both manual and digital; internal and external) that process Personal Data
- all our data processing locations, whether in, or out of country

Data Protection Rules

We shall:

Only process Personal Data which is relevant to our organisation needs

Together with our Data Subjects, keep their Personal Data up to date

Not keep Personal Data in the hope that it may become useful later on

Only grant access to the data to people who need to use it for their jobs

Protect the data from accidental loss or theft

Where required, always seek the Data Subject's consent

Where required, always seek the consent of a parent or legal guardian in respect of a Child

Only process *sensitive Personal* Data where we are legally required to do so

When communicating with our Data Subjects, always be open and transparent, using language that is easily understandable

Be aware of possible Data Subjects requests to access and manage their Personal Data and how to respond to such requests

Be aware of possible breaches (breakdowns) of security of Personal Data and how to respond to such breaches

Be aware of and respond timeously to any training and awareness programs and communications within our organisation